UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/500,311	06/28/2004	David Arditti Modiano	T2678-9156US01	9860

181 7590 04/14/2008

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
YALEW, FIKREMARIAM A	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
04/14/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

ipdocketing@milesstockbridge.com
sstiles@milesstockbridge.com

Office Action Summary	Application No.	Applicant(s)	
	10/500,311	ARDITTI MODIANO ET AL.	
	Examiner	Art Unit	
	Fikremariam Yalew	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 March 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *19,21,23-36 and 39* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *19,21,23-36 and 39* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 03/27/2008 has been entered.

2. Claims 1-18 and 37-38 were previously canceled. Claims 20,22,40 are cancelled. Claims 19,21,23-36,39 have been amended. Claims 19,21,23-36,39 are pending.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 19,21,23-36,39 are rejected under 35 U.S.C. 102(e) as being anticipated by Hopkins et al (hereinafter referred as Hopkins) US Patent 7,093,133 B2.

5. As per claim 19: Hopkins disclose a group signature device for providing a message (m) accompanied a group by a group signature (S) comprising means storing personalized data(z, Kz)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22); encryption means(B3)for producing an

encrypted text(C)(See col 6 lines 61-63 and col 8 lines 23-30),intended to be associated with said message (m),using said personalized data (z,Kz)(See col 6 lines 38-63 and col 8 lines 23-30); singing means (B6) for producing the group signature (S) with a private signature key (SK) common to all group members using the message to be signed (m) and said encrypted text (C)(See Fig 7 step 20 and col 5 lines 23-35); and means for outputting the message (m) and the group signature (S) to a checker, such that the checker, upon receiving the message accompanied by the group signature, is able to verify that message(m) is associated with the group (G) based on the group signature (S), with the identify of the member (M) of the group (G) remaining anonymous the checker(See col 2 lines 52-57 and col 5 lines 36-56).

9. As per claim 21: Hopkins discloses a group signature device further comprising means (B5) for combining the message (m) to be signed and the encrypted text (C) associated with said message (m) in the form of a concatenation of the message (m) with the encrypted text (C)(See col 6 lines 61-63 and col 8 lines 23-30 and Fig 7 steps 100,20).

10. As per claim 23: Hopkins discloses a group signature device wherein said personalized data is an identifier (z) personal to the member (M), said means for storing further includes an encryption key (K) common to all members of the group (G), and encryption means (B3) produces said encrypted text(C) using the identifier (z) and said encryption key (K) (See col 5 lines 18-35 and col 10 lines 11-38).

12. As per claim 24: Hopkins discloses a group signature device in which encryption means (B3) produces said encrypted text (C) using identifier (z) and a random number (r)(See col 7 lines 31-38 and col 10 lines 1-10).

13. As per claim 25: Hopkins discloses a group signature device wherein said personalized data is a diversified encryption key (Kz) specific to each member (M) of the group (G), and encryption means (B3) produces said encrypted text (C) using at least one data and said diversified encryption key (Kz) (See See col 5 lines 18-35 and col 10 lines 11-38).

14. As per claim 26: Hopkins discloses a group signature device wherein said data includes a random number(r) (col See col 7 lines 31-38 and col 10 lines 1-10).

15. As per claim 27: Hopkins discloses a group signature device wherein the encryption means (B3) uses a secret key encryption algorithm(K)(See 10 lines col 26-38).

16. As per claim 28: Hopkins discloses a group signature device wherein the encryption means (B3) uses one of the Rivest, Shamir, Adleman or Advanced Encryption Standard (AES) public encryption algorithms (See 10 lines col 26-38).

17. As per claim 29: Hopkins discloses a group signature device wherein the sign means (sig-B6) uses a private key signature algorithm (SK) (See 10 lines col 26-38).

18. As per claim 30: Hopkins discloses a group signature device which the private key signature algorithm is of Rivest, Shamir, Adleman(RSA) type.(See 10 lines col 26-38).

19. As per claim 31: Hopkins discloses a group signature device in which said group signature device is a portable communicating device (26)(See col 6 lines 9-18).

20. As per claim 32: the combination of David and Saito disclose a group signature device in which said portable communicating device is a smart card (26)(See col 6 lines 9-18).

21. As per claim 33: Hopkins discloses a method for secure communication of a message (m) sent by a member (M) of a group (G) using a group a signature (S) the method comprising producing the group signature (S) of the message (m) by singing, with a private signature key

(SK) common to all group members (M), a set including the message (m) and encrypted text(C) produced by using a personalized data (Z, Kz)(See col 5 lines 18-35 and col 10 lines 11-38); and outputting the message(m) along with the group signature (S)(See Fig 7 step 20)

22. As per claim 34: Hopkins discloses the method further comprising using a public key (PK) corresponding to said private signature key(SK),that the message (m) is associated with the group(G) based on the group signature (S), without identifying the member(M) of the group (G)(See col 2 lines 53-57 and col 5 lines 48-56)

23. As per claim 35: Hopkins discloses the method further comprising the steps of: decrypting the encrypted text (C) thus obtaining the personalized data (z, Kz)(see col 5 lines 38-41); and identifying the member (M) of the group (G) based on said personalized data (z, Kz)(See col 5 lines 41-56 and col 6 lines 5-18).

24. As per claim 36: Hopkins discloses the method further comprising producing a private signature key(SK) common to all members of group(G); producing personalized data (z; Kz) identifying the member (M) accepted into group (G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22); and registering said personalized data (z, Kz) with the private signature key(SK) in an electronic device personalized to said member (M) of the group (G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22)

25. As per claim 39: Hopkins discloses a group signature system for ensuring a secure communication of a message (m) sent by a member (M) of a group (G) using a group signature (S), said group signature system comprising; an electronic device configured to store a personalized data (z, Kz) identifying the member (M) of the group (G)(See Fig 2 and col 6 lines 38-56 and col 6 lines 9-22), to produce the group signature (S) with a private key (SK) common

to all group members using the message (m) and said encrypted text(C) and to output the message(m) and the group signature(S)(See Fig 7 step 20 and col 5 lines 23-35); a checker that receives that receives the message (m) accompanied by the group signature (S) output from the electronic device, said checker being configured to verify that the message (m) is associated with the group signature (G) based on the group singnature(S), the identity of the member (M) remaining anonymous to the checker(See col 2 lines 52-57 and col 5 lines 36-56); and a trusted authority configured to identify the member(M) of the group(See Fig 1 step 14)

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Fikremariam Yalew whose telephone number is 5712723852. The examiner can normally be reached on 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Moazzami Nasser can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Fikremariam Yalew Art Unit 2136
04/07/2008
FA

/Nasser G Moazzami/
Supervisory Patent Examiner, Art Unit 2136